# PERSONNEL CABINET
# DEPARTMENT OF EMPLOYEE INSURANCE
# KENTUCKY EMPLOYEES' HEALTH PLAN
# HIPAA SECURITY POLICIES

## Introduction

The Public Employee Health Insurance Program commonly known as the Kentucky Employees' Health Plan (the "Group Health Plan") is a group health plan sponsored by Personnel Cabinet, Department of Employee Insurance. (the "Plan Sponsor"). Members of the Plan Sponsor's workforce may create, receive, maintain, or transmit electronic protected health information (as defined below) on behalf of the Plan Sponsor, for plan administration functions. The Group Health Plan is administered by a third-party administrator and has one or more business associates that perform functions for the Group Health Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology For Economic and Clinical Health Act ("HITECH Act") and their implementing regulations and guidance require the Group Health Plan to implement various security measures with respect to electronic protected health information (electronic PHI).

Electronic Protected Health Information is protected health information that is transmitted by or maintained in electronic media. Protected Health Information (PHI) is the information that is subject to and defined in the Plan's privacy policies and procedures. For purposes of this Policy, PHI does not include the following, referred to this Policy as "Exempt Information":

> (1) Summary health information, as defined by HIPAA's privacy rules, for purposes of (a) obtaining premium bids or (b) modifying, amending, or terminating the Group Health Plan;
> (2) Enrollment and disenrollment information concerning the Group Health Plan which does not include any substantial clinical information; or
> (3) PHI disclosed to the Group Health Plan and/or Plan Sponsor under a signed authorization that meets the requirements of the HIPAA privacy rules.

Electronic Media means:

> (1) Electronic storage media including memory devices in computers (hard drives and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
> (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open, extranet (using Internet technology to link a business with information accessible only to collaborating parties, leased lines, dial-up lines, private networks, and the

physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission. It is the Group Health Plan's policy to comply fully with the requirements of HIPAA's security regulations.

No third-party rights (including but not limited to rights of Group Health Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Group Health Plan reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent that this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Group Health Plan. This Policy does not address requirements under state law or federal laws other than HIPAA.

**I. Security Official**

Cindy Stivers, Director of Division of Financial and Data Services, is the Security Official for the Group Health Plan. The Security Official is responsible for the development and implementation of the Group Health Plan's policies and procedures relating to security, including but not limited to this Policy.

**II. Risk Analysis**

The Group Health Plan has no employees. All of the Plan's functions, including creation and maintenance of its records, are carried out by employees of the Plan Sponsor and by business associates of the Plan. The Group Health Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Plan Sponsor, the third-party administrator and other business associates. Accordingly, the Plan Sponsor and business associates create and maintain all of the electronic PHI relating to the Plan, own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit electronic PHI relating to the Plan, and control their employees, agents, and subcontractors who have access to electronic PHI relating to the Plan. The Group Health Plan has no ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the Plan.

That ability lies solely with the Plan Sponsor, the third-party administrator and other business associates. Because the Group Health Plan has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Plan Sponsor, the third-party administrator and other business associates affecting the security of Group Health Plan electronic PHI, and the Plan Sponsor, the third party administrator and other business associates have undertaken certain obligations relating to the security of electronic PHI that they handle in relation to the performance of

administrative functions for the Plan, the Plan's policies, and procedures, including this Policy, do not separately address the following standards (including the implementation specifications associated with them) established under HIPAA that are set out in Subpart C of 45 CFR Part 164:

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

The HIPAA security policies and procedures of the Plan Sponsor and the third-party administrator and other business associates for electronic PHI of the Group Health Plan for the standards listed above are adopted by the Group Health Plan.

The Department of Employee has created a separate document entitled "HIPAA Security Policies and Practices" addressing the Plan's policies and procedures.

**III. Risk Management**

The Group Health Plan manages risks to its electronic PHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level, taking into account the following:

- The size, complexity, and capabilities of the Group Health Plan;
- The Group Health Plan's technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and,
- The criticality of the electronic PHI potentially affected.

Based on risk analysis discussed in section II, the Group Health Plan made a reasoned, well-informed and good-faith determination on the implementation of the HIPAA security regulations that it need not take any additional security measures, other than the measures set forth herein and the measures of the Plan Sponsor, the third-party administrator, and other business associates, to reduce risks to the confidentiality, integrity and availability of electronic PHI.

## IV. Group Health Plan Document

The Group Health Plan document shall include provisions requiring the Plan Sponsor to:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the Plan Sponsor creates, receives, maintains, or transmits on behalf of the Group Health Plan (the Plan electronic PHI);
- ensure that reasonable and appropriate security measures support the Group Health Plan document provisions providing for adequate separation between the Group Health Plan and the Plan Sponsor (which were adopted as described in the Group Health Plan's privacy policy);
- ensure that any agents or subcontractors to whom the Plan Sponsor provides Plan electronic PHI agree to implement reasonable and appropriate security measures to protect the Group Health Plan electronic PHI; and
- report to the Security Official any security incident of which the Plan Sponsor becomes aware.

## V. Disclosures of Electronic PHI to Third-Party Administrator and Other Business Associates

A business associate is an entity (other than the Plan Sponsor), such as a third-party administrator, that:

- performs or assists in performing a Group Health Plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI. The Group Health Plan permits the third-party administrator and other business associates to create, receive, maintain, or transmit electronic PHI on its behalf. The Group Health Plan has obtained or will obtain satisfactory assurances from all business associates that they will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract containing all of the requirements of the HIPAA security regulations and specifically providing that the business associate will:
- implement administrative, physical, and technical safeguards and documentation requirements that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the Group Health Plan (the Contract electronic PHI);
- ensure that any agents or subcontractors to whom the business associate provides Contract electronic PHI agree to implement reasonable and appropriate security measures to protect the Contract electronic PHI;
- report to the Group Health Plan any security incident of which the business associate becomes aware;

• take required steps with respect to breach notification requirements; and
• authorize termination of the contract by the Group Health Plan if the Group Health Plan determines that the business associate has violated a material term of the contract.

## VI. Breach Notification Requirements

The Group Health Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Group Health Plan or one of its business associates discovers a breach of unsecured PHI.

## VII. Documentation

The Group Health Plan's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of Group Health Plan electronic PHI, and any changes to policies or procedures will be documented promptly. Except to the extent that they are carried out by the Plan Sponsor or business associates, the Group Health Plan shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented (including amendment of the Group Health Plan document in accordance with this policy, for example). Policies, procedures, and other documentation controlled by the Group Health Plan may be maintained in either written or electronic form. The Group Health Plan will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

The Group Health Plan will make its policies, procedures, and other documentation available to the Security Official and the Plan Sponsor, the third-party administrator and other business associates or other persons responsible for implementing the procedures to which the documentation pertains.